STATE OF MONTANA
Montana Information Security Advisory Council
Best Practices Workgroup

Identification and Authentication Policy Overview

Version 1.1
12-21-2016

1. Purpose

This document provides a summary and overview of the Identification and Authentication policies for the State of Montana.

2. Policy

Identification and Authentication applies to the following controls found within the Information Security Policy.

a. Information Security Policy
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

b. Information Security Policy – Appendix A
  - Identification and Authentication (IA)

3. Policy Statement for Identification and Authentication

Each Agency shall manage identities and credentials for authorized devices and users.

3.1 Standards for Authentication

Each agency shall provide a means to identify and authenticate authorized devices and users utilizing one of the following methods:

1) Authentication of devices and users inside of the State Network (SummitNet)

a. Microsoft Active Directory is the standard for providing unique identification and authentication of authorized devices and users. Devices primarily include all network attached equipment. Users primarily include state employees but may also include non-organizational attached individuals performing state business.

b. ePass Montana is an alternative standard for providing unique identification and authentication of users. These users primarily include non-organizational attached individuals but may include state employees and other individuals performing state business.

c. Exceptions - Non-conforming devices and users which are unable to utilize either Active Directory or e-Pass for identification and authentication shall apply for an exception. Examples include database applications and legacy systems such as mainframe.

2) **Authentication of users to systems that reside outside of SummitNet.** Cloud or vendor hosted solutions/systems shall identify and authenticate users by utilizing the following methods:

a. Microsoft Active Directory Federation Services – a standards based service that allows the secure sharing of identity information between trusted business partners. Users of this method primarily include state employees but may also include non-organizational attached individuals performing state business.

b. ePass Montana is an alternative standard for providing unique identification and authentication of users. These users primarily include non-organizational attached individuals but may include state employees and other individuals performing state business.

c. Exceptions - Non-conforming users which are unable to utilize either Active Directory Federation Services or ePass for identification and authentication shall apply for an exception.

3.2 Standards for User Identification

The State of Montana permits User Identification to State information systems according to the following requirements:

- User accounts must utilize a password that has a minimum of 8 characters and contains:
  - At least one lower case
  - At least one upper case
  - At least one number or special character
- Agency documented provisioning and de-provisioning standards
- Change of user account password upon first login
- Forcing user account password changes every 60 days.
- A warning of password expiration must be seven days or greater for systems that support this capability.
- The user account password cannot be the same as the User Identification.
- All vendor-supplied default passwords shall be changed by system administrators before any computer or system is used in production.

- Systems shall:
  - require unique User Identification for each account
  - prohibit clear-text transmission and storage of passwords.
  - initiate a session lock after 15 minutes of inactivity.
  - mask authentication information during the authentication process
  - not allow anonymous authentication
  - prohibit the use of local user accounts excluding local Administrator accounts.
  - assign an account manager to every unique user identification.
  - prohibit password reuse for six (6) generations
  - Minimum age of password – 24 hours

  The user account shall be locked after six attempts of providing the incorrect password, the account shall be locked for a period of at least 8 hours or until an administrator unlocks the account.

Commented [FJ1]: Best Practices recommends added this to IA-5 in the Information Security Policy. This is the current recommendation from IRS Publication 1075 and Microsoft

Commented [FJ2]: Best Practices recommends changing this in the Information Security Policy from 8 hours to IRS Publication 1075 recommendation of 15 minutes.

- Passwords, tokens, smart cards, etc. associated with user identifications shall not be shared, written down, or easily accessible by unauthorized individuals.
- User accounts shall be disabled if inactive for ninety (90) days

3.3 Elevated/Privileged/Administrative/SU Accounts

An Elevated/Privileged/Administrative/SU account is any account that has been granted administrator level privileges. The State of Montana permits these accounts for identification to State information systems according to section 3.2 requirements with the following additional requirements:

- Elevated/Privileged/Administrative/SU accounts shall be assigned to users that require elevated rights or access to perform administrative job functions.
- Elevated/Privileged/Administrative/SU Accounts are to be used only for administrative tasks.

Commented [FJ3]: Best Practices workgroup had a discussion around this bullet. Clarification is needed on the intent; during the Best Practices workgroup meeting the meaning was interpreted differently.

- Elevated/Privileged/Administrative/SU accounts are assigned after a signed Privileged User Responsibilities form is on file.
- Elevated/Privileged/Administrative/SU accounts shall be logged using an access log or an auditing application. Logs must contain the following information:
  - Date
  - Time
  - Network address
  - User ID
  - Description of work
- The use of multifactor authentication is required for any account(s) that has elevated rights.
- Passwords for Elevated/Privileged/Administrative/SU Accounts should be at least 15 characters long and contains alpha, numeric, special characters, and capital letters.

Commented [FJ4]: This is DOA SITSD Policy. It is recommended by the Best Practices workgroup to update the POL-Information Security Policy in IA-5 to include a section for privileged accounts

Certain system tasks require the use of other elevated privilege accounts. When possible, employees using this account must first log on with their general user identification and then use the Elevated/Privileged/Administrative/SU account.

3.4 Service Accounts

A service account is an account that does not correspond to an actual person. These are accounts that services use to access resources they need to perform their activities. The State of Montana permits service accounts identification to State information systems according to section 3.2 requirements with the following additional requirements:

- Service Accounts shall be unique to the service/application.
- Passwords for Service Accounts can be set so that they do not age or expire if they have a password that is at least 15 characters long and contains alpha, numeric, special characters, and capital letters.
- Service Accounts must be reviewed to ensure that they are configured to run with the least number of privileges needed by a service.
- Service Account information shall not be stored in readable format i.e. batch files, scripts, plain text, etc.
- All Service Accounts must be documented and stored in a secured fashion as follows:
  - ID name
  - Password
  - Date the account was established
  - Purpose of the account
  - Name of server(s) it connects to
  - Level of access for the account
  - Account managers shall review service accounts annually.

3.5 Network Attached Device Authentication and Identification

All internal networks shall be configured such that they can prevent and/or detect attempts to connect from unauthorized devices. All devices gaining access to the state network shall be authenticated to a device management system.

3.6 Certificate based authentication

The State of Montana requires the validation of certificates and the mapping the identity to the user account

3.7 Token-based authentication

The State of Montana information systems that use hardware token-based authentication shall employ mechanisms that satisfy public key Infrastructure (PKI) requirements.

4. Relevant Policies

   a. Identification and Authentication Policy
   b. Service and Elevated Accounts Policy
   c. Secured eGovernment Service Access Policy
   d. Appendix A – Baseline Security Controls

5. Compliance

   Compliance shall be evidenced by implementing these requirements as described above. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to these requirements are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.